



**AUDIT OF THE COMPUTER CONTROLS
FOR THE
KENTUCKY DIRECT SALES SYSTEM
OF THE
DEPARTMENT OF FISH AND WILDLIFE RESOURCES**

**For the Period of
March 1, 1997 through February 28, 1998**

**EDWARD B. HATCHETT, JR.
AUDITOR OF PUBLIC ACCOUNTS
WWW.STATE.KY.US/AGENCIES/APA**

**144 CAPITOL ANNEX
FRANKFORT, KY 40601
TELE. (502) 573-0050
FAX (502) 573-0067**

CONTENTS

	<u>Page</u>
<u>TRANSMITTAL LETTER</u>	1
<u>INDEPENDENT ACCOUNTANT'S REPORT</u>	3
<u>COMMENTS AND RECOMMENDATIONS</u>	5



EDWARD B. HATCHETT, JR.
AUDITOR OF PUBLIC ACCOUNTS

March 2, 1999

To the People of Kentucky
Honorable Paul E. Patton, Governor
Ann R. Lata, Secretary
Tourism Development Cabinet
Tom Bennett, Commissioner
Department of Fish and Wildlife Resources
Bob Bates, Director
Administrative Services

Re: Information Technology Audit

Ladies and Gentlemen:

I am pleased to transmit herewith the report of our audit of the computer system controls applicable to the Kentucky Direct Sales System (KDSS) of the Department of Fish & Wildlife Resources (DFWR) for the year ended February 28, 1998.

Our audit was conducted in accordance with generally accepted governmental auditing standards, and attestation standards established by the American Institute of Certified Public Accountants. We conducted this audit for the purpose of issuing an opinion concerning the adequacy of the computer system controls established by DFWR management as identified in their management assertion letter dated March 31, 1998. The DFWR management presented assertions that they had established adequate system controls over computer operations and organization, physical and logical security, business recovery planning, program modification control data authorization, data validity, data completeness, and data accuracy.

In our opinion, management's assertion that, for the fiscal year ended February 28, 1998, DFWR designed and maintained adequate computer system controls for KDSS to achieve the specified control objectives is fairly presented in all material respects. However, we did note certain immaterial weaknesses.

To the People of Kentucky
Honorable Paul E. Patton, Governor
Ann R. Lata, Secretary
Tourism Development Cabinet
Tom Bennett, Commissioner
Department of Fish and Wildlife Resources
Bob Bates, Director
Administrative Services
March 2, 1999
Page 2

Our audit revealed the absence of formal logical security policies, and some minor weaknesses with logical access security procedures. Additionally, no formal business recovery plan had been developed. Our audit also found that at the time of our fieldwork, DFWR had not completed the necessary procedures to ensure KDSS was ready for year 2000 processing. Finally, we noted weaknesses in accounting procedures which resulted in the failure to identify discrepancies in revenue recorded within KDSS and the Statewide Accounting and Reporting System (STARS). Specifically, DFWR recorded license sales revenue totaling \$37,412,530.90 in KDSS for the period January 1, 1996 through April 1, 1998, which exceeded the license sales revenue recorded in STARS by \$457,831.74 or 1.22%. Discrepancies between these two systems involved several pay-in-vouchers and related journal vouchers. Specifying the cause for the variances for each document was beyond the scope of this audit. We understand the agency's personnel will resolve the revenue variance issue.

On behalf of our audit team consisting of Tony Hutchins, EDP Audit Manager, and staff member Gary LeMaster, I wish to thank the employees of the DFWR for their cooperation during the course of our audit. If you have any questions concerning this report, please contact Brian Lykins, Director, Division of Examination and Information Technology.

Very truly yours,

A handwritten signature in dark ink, appearing to read "Ed Hatchett", with a stylized flourish at the end.

Edward B. Hatchett, Jr.
Auditor of Public Accounts

EBHJr:kct



EDWARD B. HATCHETT, JR.
AUDITOR OF PUBLIC ACCOUNTS

To the People of Kentucky
Honorable Paul E. Patton, Governor
Ann R. Lata, Secretary
Tourism Development Cabinet
Tom Bennett, Commissioner
Department of Fish and Wildlife Resources
Bob Bates, Director
Administrative Services

Re: Information Technology Audit

Ladies and Gentlemen:

Independent Accountant's Report

We have examined management's assertion, included in its representation letter dated March 31, 1998, that DFWR had designed and maintained adequate general and application system controls, as they apply to KDSS, for the fiscal year ended February 28, 1998. Our examination was made in accordance with generally accepted governmental auditing standards as promulgated by the Comptroller General of the United States, and in accordance with attestation standards established by the American Institute of Certified Public Accountants.

We restricted our examination to the system controls that were applicable to KDSS as of February 28, 1998. Any projection of such information to the future is subject to risk that, because of change, the controls tested may no longer represent the computer system control structure in existence. The potential effectiveness of tested controls at DFWR is subject to inherent limitations and, accordingly, errors or irregularities may occur and not be detected.

In our opinion, management's assertion that, for the fiscal year ended February 28, 1998, DFWR designed and maintained adequate computer system controls for KDSS to achieve the specified control objectives is fairly presented in all material respects. However, we did note certain immaterial instances of noncompliance, which are presented in the comments and recommendations section of this report.

To the People of Kentucky
Honorable Paul E. Patton, Governor
Ann R. Lata, Secretary
Tourism Development Cabinet
Tom Bennett, Commissioner
Department of Fish and Wildlife Resources
Bob Bates, Director
Administrative Services

This report is intended solely for the use of the Fish and Wildlife Commission, management of DFWR, the Auditor of Public Accounts, the Commonwealth of Kentucky, other agencies within the Commonwealth of Kentucky, and the independent auditors of the agencies.

Respectfully submitted,

A handwritten signature in dark ink, appearing to read "Ed Hatchett", written in a cursive style.

Edward B. Hatchett, Jr.
Auditor of Public Accounts

Fieldwork completed –
January 8, 1999

COMMENTS AND RECOMMENDATIONS

COMMENTS AND RECOMMENDATIONS

1) The Department of Fish and Wildlife Resources Should Improve Logical Access Security

DFWR's KDSS resides on a local area network (LAN) platform and employs a Novell Netware operating system. Novell Netware security is used to control access to the LAN. An authorized user ID and password are required to access the DFWR LAN. In addition, Oracle and PowerBuilder software provide a secondary level of access control security for the KDSS computer programs and data files. Our examination of the DFWR access security controls revealed the following weaknesses:

- Formal access request forms were not completed to request and document access to the LAN. The administrator assigns access based on telephone discussions or other informal means.
- Each user was not required to sign a security agreement to acknowledge his/her responsibility to maintain data confidentiality and to use agency computing equipment and data solely for business purposes.
- Formal procedures were not established requiring the LAN administrator to be notified when employees with DFWR LAN access transfer or terminate employment. Our procedures revealed that of the 24 active user IDs with access to KDSS at the time of our audit, 4 were terminated employees, and 5 transferred to positions not requiring KDSS access. We observed no evidence that any of these nine user IDs were used to access KDSS after the employees' termination or transfer. At our recommendation, the LAN administrator disabled these nine user accounts.
- Netware security allows the LAN administrator to establish certain user account restrictions that require a user password, and specify control of the passwords. Our testing identified that restrictions were not implemented to require unique passwords for any KDSS users. Also, a reasonable password expiration period was not established for the LAN administrator's user account, which has supervisory level access.

Approximately one hundred users access the DFWR LAN. During the period under examination, there were twenty-four users who could access the KDSS application. Approximately \$17.2 million dollars in revenue was processed through the KDSS system in fiscal year 1998. The propriety of system access levels granted cannot be ensured without properly documented access requests that are approved by the employee, the employee's supervisor, and the security coordinator. Failure to promptly revoke user access when personnel terminate or transfer created an unnecessary vulnerability for DFWR. This increases the possibility of unauthorized access and alterations to DFWR programs and data. The failure to restrict passwords by requiring forced expirations and a unique password for each user increases the likelihood that passwords can be discovered by unauthorized users.

1) The Department of Fish and Wildlife Resources Should Improve Logical Access Security (continued)

The accountability and audibility of system access can only be achieved through documented request and approval procedures. The level of system access granted should be restricted to computer programs and data necessary for the employee to perform his/her assigned job duties. System access should be revoked or adjusted when employees transfer or terminate employment. Employees should be required to sign security agreements to ensure each individual is aware of his/her rights and responsibilities concerning the use of agency computing resources. Finally, adequate account restrictions should be placed on user accounts to ensure the integrity of password controls.

Recommendation

The DFWR logical access security procedures should be enhanced. DFWR should develop a formal system access request form. The form should be completed to obtain or modify employee access to computing resources and should identify the applications and the level of access required. The employee's supervisor should sign the access request form, and the LAN administrator should date the form when the access is granted. Additionally, employees should be required to sign a security agreement concerning the use of DFWR computing resources. Further, DFWR should implement personnel procedures to ensure the LAN administrator is notified of employee transfers or terminations so that system access can be adjusted accordingly. Finally, account restrictions should be improved by requiring unique passwords for LAN users, and the LAN administrator's account should be changed to require password expiration every thirty days.

Agency Response

We will develop a formal access request form that will be completed to obtain or alter employee access to the network resources and will identify the applications and the level of access required. Employees will be required to sign a security agreement concerning the use of network resources. Personnel procedures will be created to inform the LAN administrator of employee transfers or terminations. Unique passwords will be required for LAN users. The LAN administrator's account will be changed to require password expiration every thirty days.

2) The Department of Fish and Wildlife Resources Should Develop a Disaster Recovery Plan

DFWR did not have a business recovery plan in effect during the fiscal year 1998. Adequate backup and recovery policies and procedures were put in place to ensure the backup of critical system and data files for KDSS. However, a complete business recovery plan was not developed. Further, DFWR did obtain adequate insurance coverage for the LAN computer equipment through State Risk and Insurance Services. However, they did not obtain insurance coverage for approximately 302 terminals and 296 printers that were stored in either the DFWR Administrative Services Building, or at various county clerks' offices.

2) The Department of Fish and Wildlife Resources Should Develop a Disaster Recovery Plan (continued)

Not having a business recovery plan increased the possibility of loss due to excessive recovery time and increased costs, and the disruption of DFWR processing capabilities. DFWR inventory records revealed they have approximately 302 agent terminals and 296 agent printers in inventory not currently in use by agents. These terminals and printers were valued at approximately \$153,000. In the event of a disaster, the agency would not be able to recover the replacement value for this equipment.

Good management practices minimize risks through planning. The goal of a business recovery plan is to improve preparedness at minimal cost using available resources. Additionally, computer equipment should be insured to facilitate continued operations in the case of loss.

Recommendation

We recommend DFWR continue efforts to update their computer equipment insurance to include the agent terminals and printers they maintain in inventory at DFWR and the various county clerks' offices. The location of these items can be listed as "various" when submitted to the State Risk and Insurance Services to ensure coverage, based on our discussions with State Risk and Insurance. Additionally, we recommend a formal business recovery plan be developed for the DFWR computing facilities. This plan should address recovery concerns such as:

- Disaster definitions
- Identification of emergency personnel and phone numbers
- Identification of mainframe gateways and procedures for replacement
- Identification of critical data and software, and an explanation of backup procedures (or refer to backup procedures noted in other manuals)
- Listing of vendor contacts with whom agreements were made for obtaining emergency equipment replacement
- Specific procedures to be followed for business recovery during various levels of disaster or downtime
- Backup or manual procedures to be followed for business continuity in the case of extended disruption
- Training of emergency personnel
- Periodic testing of the recovery plan

2) The Department of Fish and Wildlife Resources Should Develop a Disaster Recovery Plan (continued)

Agency Response

We agree that a formal business recovery plan is needed. Most of the components are in place, just not formalized. Our Information Systems section has a list of emergency personnel and their telephone numbers, a list of gateways and replacement procedures, a list of software, and a document of backup and restoration procedures. The Help Desk has a series of procedures for recovery of agents' sales records. The two KDSS sections, Information and Help Desk, will work together to formalize a business recovery plan.

Since the supply of terminals stored in the Administrative Services building were not covered as contents of the building, we have taken steps necessary to add them to our computer policy. Over time we have reduced the number of county clerks with spare terminals. Our ability to replace terminals from the Frankfort office is very effective. The balance of the terminals in the county clerk offices need a software revision and will be called in for an update process very soon. These terminals will not be returned to the county clerks. Once they are re-worked and ready for issue, we will simply add them to our main inventory in Frankfort.

3) The Department of Fish and Wildlife Resources Must Modify Their Computer Systems To Ensure They Can Process Year 2000 Data

DFWR did not complete the modifications necessary to make KDSS year 2000 compliant. DFWR contracted with COMPAQ Services (COMPAQ) in June 1998 to conduct a year 2000 compliance analysis. COMPAQ specifically determined which computer equipment and hardware changes were needed for the system to properly process four digit date fields, and comply with year 2000 concerns. Many of the KDSS components were already compliant, and other necessary hardware changes were made. However, modifications or upgrades were still needed for major software and hardware components utilized by KDSS. The major KDSS components that remain non-compliant rely on outside vendors to supply hardware or software upgrade alternatives, or software patches to make the components compliant. Many KDSS component vendors were still working on this process.

Additionally, although DFWR has completed their year 2000 compliance analysis, they have not submitted adequate inventory and assessment information as required by the Department of Information Systems (DIS).

The year 2000 calculation is a problem associated with applications designed to save space by eliminating the "19" as the century in dates. If these systems process data with the numbers "00" to represent the year, they may produce incorrect results or become totally dysfunctional because the systems may interpret this input as the year 1900 instead of 2000.

3) The Department of Fish and Wildlife Resources Must Modify Their Computer Systems To Ensure They Can Process Year 2000 Data (continued)

It is critical that all KDSS related hardware and software components be updated or replaced so that they comply with year 2000 processing requirements.

Recommendation

We recommend that DFWR complete and submit the necessary year 2000 documentation as requested by DIS. Further, DFWR management should take the necessary steps to ensure KDSS is year 2000 compliant. We recommend management ensure all required hardware and software modifications or replacements be accomplished by December 31, 1998, and modifications to the system are properly tested.

Agency Response:

Y2K documentation has been submitted to KIRM. As part of our Y2K plan, KDSS will be fully Y2K compliant by May 1999.

4) The Department of Fish and Wildlife Resources Should Develop Adequate Written Security Policies And Procedures Identifying Management And User Responsibilities For System Security

The DFWR did not develop formal policies and procedures to identify management and user responsibilities for system security. DFWR did follow certain procedures to secure system access based on user needs. However, formal written documentation of user and security administrator responsibilities, policies, and security procedures was not developed.

The failure to document existing policies could lead to a lack of understanding by management and users, and result in a failure to comply with security policies such as the issuing, deleting, and sharing of user IDs. Failure to comply with security policies could lead to unauthorized data or program modification, destruction of assets, and interruption of services.

For security to be effectively implemented and maintained, written policies and procedures should be developed. This provides the security framework used to educate management and users of their security responsibilities. Further, formalized security policies provide continuity for policy implementation and illustrate management's concern for strong system security.

4) The Department of Fish and Wildlife Resources Should Develop Adequate Written Security Policies And Procedures Identifying Management And User Responsibilities For System Security (continued)

Recommendation

We recommend the DFWR develop detailed written policies to establish standards for system security and procedures to be followed by the security administrator and system users. At a minimum, these security policies should:

- Define the duties and responsibilities of the security administrator.
- Develop formal procedures for notifying the security administrator of terminations or transfers of employees with system access.
- Outline a security awareness program covering training, new hire orientation, and confidentiality statements. Periodic communication of the security policy to all employees should be required. Employees need to be made aware of their responsibility to ensure the proper use and confidentiality of data, user logon IDs, and passwords.
- Define procedures for maintaining adequate physical control over system resources such as keeping doors locked, if applicable, and logging off terminals when employees leave the workstation.
- Define general procedures to be followed for conducting inquiries when it appears system security or data confidentiality was comprised, and define formal disciplinary actions to be taken against security violators.
- Define rules and responsibilities relating to access of programs and data files including procedures for requesting and processing modifications, additions, and deletions to system access.

Agency Response

Fish & Wildlife is as concerned about proper security as anyone. A network analyst was employed for that reason. The widespread use of technology, especially email, and the increase in employees have put great demands on our information systems staff. Up until now, we have not required formal procedures for our security process due to the low rate of department employee turnover. The changes have been minimal and the processes manageable. However, we have grown to the point where formal policies and procedures will be beneficial. We will develop formal written policies, procedures, and responsibilities for system security.

5) The Department of Fish and Wildlife Resources Should Ensure Kentucky Direct Sales System Transactions Are Properly Reflected in STARS

The DFWR, Administrative Services Division, did not establish documented policies and procedures to ensure transactions were properly reconciled between KDSS and STARS.

5) The Department of Fish and Wildlife Resources Should Ensure Kentucky Direct Sales System Transactions Are Properly Reflected in STARS (continued)

A review of the pay-in voucher (PV) activity for KDSS and STARS revealed discrepancies between the revenue recorded within the two systems. Specifically, DFWR recorded license sales revenue totaling \$37,412,530.90 in KDSS for the period January 1, 1996 through April 30, 1998, which exceeded the license sales revenue recorded in STARS by \$719,515.94. However, further review revealed that three PVs recorded in KDSS were not posted to the proper PV number. In one instance on July 11, 1997, KDSS revenues were recorded in the amount of \$53,116.10 on PV074926. However, this PV number was changed by Administrative Services Division personnel before it was forwarded to the Finance Cabinet's Division of Accounts (DOA). The transaction was posted in STARS on PV051201 on July 31, 1997. We found two other similar occurrences where the moneys involved were \$48,154.20 and \$160,413.90, respectively. The moneys were deposited and recorded in STARS properly, but recorded under the wrong PV within KDSS. Therefore, in these instances discrepancies existed between the two systems only because different PV numbers were used in each system. After consideration of these three PVs, the remaining variance was \$457,831.74 or 1.22%.

Our audit noted instances of incorrect Journal Voucher (JV) entries that caused net PV amounts to be overstated or understated. For instance, PV100478 is overstated in KDSS by \$61,568.60, PV100482 is understated in KDSS by \$8,059.45, PV100484 is understated in KDSS by \$43,261.85, and PV100485 is understated in KDSS by \$10,247.30. These variances occurred because incorrect JV entries were applied to the PVs in STARS. These variances offset each other and they were not included in our noted \$457,831.74 variance.

Our audit also found that DFWR personnel sometimes manually changed PV numbers electronically generated in KDSS before they were forwarded to DOA for posting. This caused discrepancies between KDSS and STARS posting of specific PV numbers. Further, we found that DFWR personnel incorrectly identified PV numbers that DOA personnel needed to generate failed EFT JVs. These JVs reduce the original amount of revenue recorded when the revenue was not actually collected due to insufficient vendor/agent funds. This caused JVs for failed EFTs to be posted against the wrong PVs in STARS. DFWR procedures for recording failed EFT amounts are based on actual bank reports. Therefore, it is understandable why STARS data may vary from KDSS data in cases where DOA was provided the incorrect PV number for JV purposes.

Administrative Services Division personnel have not yet determined the reasons for the remaining variance. We did note JV entries made which were confusing and could not be explained by agency personnel at the time of our audit. DFWR procedures established to reconcile the KDSS activity with STARS did not reveal these variances. However, it is likely that the remaining variance is due to errors in recording PV and JV activity similar to the transactions noted above. Specifically identifying each and every one of the instances that caused the variance is beyond the scope of our review.

5) The Department of Fish and Wildlife Resources Should Ensure Kentucky Direct Sales System Transactions Are Properly Reflected in STARS (continued)

Finally, the policies and procedures established by DFWR management to ensure KDSS revenue activity was reconciled to STARS were not performed on a timely basis. At the time of our fieldwork, these reconciliation's had not been performed for the previous five months. Further, DFWR personnel were not adequately trained to query the necessary STARS information.

Policies and procedures should be established to ensure that revenues and related adjustments are properly recorded and reported to STARS. Also, the net revenue within KDSS should be reconciled with STARS to ensure proper financial reporting.

Recommendation

We recommend DFWR management ensure that procedures established to reconcile net KDSS revenues to STARS be completed in a timely and consistent manner. Those procedures should be expanded to ensure any JV activity relating to KDSS is properly recorded in STARS, and that adjustments to revenue are applied to the appropriate PV. We further recommend DFWR continue to reconcile the variances between KDSS and STARS identified in our audit, and take the actions necessary to ensure revenue is recorded accurately. DFWR management should train personnel to query STARS and KDSS to generate reports to assist with the reconciliation process. Finally, we recommend that DFWR generate the journal vouchers for failed electronic fund transfers, as opposed to preparing those documents in DOA. This may eliminate the confusion concerning the transactions recorded on those documents.

Agency Response

During implementation of KDSS, the department experienced some major personnel changes. Both the Licensing Section and the Accounting Section were impacted by these changes. The accounting section which normally reconciled STARS accounts changed several processes and was unable to keep up with the workload. Thanks to this audit, some deficiencies were noted and some processes reinstated. Additionally, new processes were created in KDSS to monitor timeliness of deposits to the Fish & Game Account and track information on NSF journal vouchers. Although we are not authorized to process journal vouchers for NSF's, we have set up a tracking system in house to eliminate the possibility of duplication. A new accounting section supervisor was hired on July, 1998. She and her staff are working to finish the backlog and have systems operating on a current basis. Her training of the accounting section staff and procedures for control will assure a reconciliation of revenues on a timely basis.

We have contacted the Treasurer's Office concerning several PV's that had posting problems and are in the process of correcting these errors. In some instance, the account clerk processing the PV simply typed two documents on the same day and reversed entries. She has been instructed to double check for a correct match.

5) The Department of Fish and Wildlife Resources Should Ensure Kentucky Direct Sales System Transactions Are Properly Reflected in STARS (continued)

Agency Response (continued)

Implementation of the MARS accounting system will provide a better way of handling all of these processes. We will have a better control of both deposits and journal vouchers. MARS includes tracking systems, which can be used for KDSS. This will eliminate the need for our auxiliary systems.